Количество кибератак на юристов будет расти

04.09.2016 ИНТЕРВЬЮ НОВОСТИ КОМПАНИЙ

В преддверии конференции по кибербезопасности мы побеседовали с одним из ее спикеров Кириллом Бельским, партнером «Коблев и партнеры», о важности защиты конфиденциальной информации в юридическом бизнесе, стоимости такой защиты и о плане действия «на

черный день».

Что дороже: репутация фирмы или затраты на кибербезопасность?

В апреле 2016 г. в результате компьютерной атаки фактически была уничтожена международная юридическая фирма Mossack Fonseca – в сеть попало более 11,5 млн документов, свидетельствующих о том, как сотни богатых и влиятельных людей использовали офшорные схемы для уклонения от налогов и сокрытия незаконных доходов. Помимо этой, безусловно, самой громкой истории, повлекшей за собой даже отставку высших должностных лиц государств, западная юридическая пресса сообщает о великом множестве атак на компьютерные системы крупных юридических фирм. В таких условиях для юристов, обслуживающих серьезные проекты, квалифицированная забота о кибербезопасности переходит в разряд жизненно важных вопросов.

Какова сегодня главная угроза для кибербезопасности юридических фирм в России?

Информация о клиентах – ценный актив юридической фирмы, на который может быть направлена кибератака. С каждым годом количество атак на юристов будет расти, поскольку они являются носителями крайне ценной высококонцентрированной информации о финансах клиентов, планируемых и совершенных ими сделках, коммерческой тайны, ноу-хау, доказательств, способных развалить любое дело, переписки, содержащей персональную информацию, которая может быть использована для компрометации, шантажа и пр.

Выгодоприобретателями атак могут быть мошенники, охотники за инсайдом, недобросовестные конкуренты в бизнесе и политике, правоохранительные органы и спецслужбы. В отдельную группу принято выделять так называемых хактивистов – лиц, использующих компьютерные сети для распространения той или иной идеологии (например, группировки Anonymous и «Шалтай-Болтай»). На мой взгляд, в действительности любые хактивисты состоят на службе в одной из перечисленных групп.

Обеспечить абсолютную безопасность компьютерных систем юридической фирмы в

настоящее время не представляется возможным. Специалисты шутят по поводу того, что все мы рано или поздно станем жертвами хакеров и будем делиться на две группы: на тех, кто узнал, что их атаковали, и на тех, кому об этом неизвестно.

Ваша фирма занимается в основном сопровождением уголовных дел. Усложняет ли это задачу обеспечения кибербезопасности и придает ли ей важности?

В последние годы значительная часть высокобюджетных хозяйственных споров влечет за собой шлейф уголовных дел, нередко откровенно заказных, возбуждаемых с целью оказать давление и путем проведения обысков и выемок получить доступ к ключевой информации. Работа адвоката в области разрешения споров интересна погружением в бизнес клиента, то есть в новые области знания. Несколько лет назад к нам обратился крупный международный производитель оборудования. Сотрудник российского офиса этой фирмы, преодолев систему защиты, скачал ценную информацию и передал ее конкурентам в качестве бонуса при трудоустройстве. В рамках внутреннего расследования, проводимого совместно с профессионалами в области IT-безопасности, мы много узнали о киберугрозе и способах противодействия ей. Впоследствии эти знания и комплекс мер по формированию системы защиты информации помогли нам успешно пережить несколько атак, за которыми стояли процессуальные и внепроцессуальные оппоненты.

Во сколько обходится кибербезопасность вашей фирме?

Наша фирма относится к бутиковому типу, у нас не так много компьютеров, поэтому ежегодные расходы на кибербезопасность составляют не более 10% в структуре расходов, не связанных с оплатой труда. Затраты делятся на две группы: первая – это единоразовый первоначальный аудит и выстраивание системы кибербезопасности, вторая – регулярные плановые и внеплановые проверки. По нашим стандартам, проверку на уязвимость от внешних вторжений должны проходить все подключенные к Интернете компьютеры и внутренние сети (настольные и портативные компьютеры, смартфоны, серверы, принтеры, VOIP телефоны).

Кто в вашей фирме задает правила IT-безопасности: управляющий партнер или айтишник?

Цели и задачи в области компьютерной безопасности нашего бюро устанавливают старшие партнеры, а методы достижения целей предлагают специалисты. Качественное обеспечение данного направления в немалой степени облегчается тем, что в ходе работы по многим проектам наших доверителей мы находимся на передовой в самых ожесточенных стадиях конфликтов и сталкиваемся с наиболее прогрессивными практиками нападения и защиты. Опыт партнеров бюро в этой области позволяет предупреждать многие проблемы, а не устранять их последствия. Например, систематическая проверка устойчивости бюро к кибератакам уже давно стала правилом, неукоснительное выполнение которого следует принимать как данность, так же как регулярное прохождение медицинского осмотра.

Еще хочу отметить, что важнейшим элементом обеспечения безопасности бюро является постоянная бдительность (и даже подозрительность), которую мы прививаем всем нашим сотрудникам. Слишком часто приходится наблюдать ситуации, когда главным доказательством по уголовному делу становится компьютер, на мониторе которого был наклеен стикер с паролем, или оставленная «про запас» флешка с финансовой документацией, которую было предписано уничтожить.

Имеется ли у вашей фирмы план действий на случай повреждения или пропажи данных в результате кибератаки, и, если да, то включено ли в него информирование клиентов?

Такой план у нас, конечно же, есть, однако было бы неразумным описывать его детали на страницах популярного издания. Разумеется, мы проинформируем клиента об атаке и в случае утечки данных представим ему перечень похищенных или поврежденных сведений. Но все же мы надеемся, что этого не случится.

Требуется ли для создания стандартов кибербезопасности вмешательство объединений (ФПА, АЮР и пр.), или юристы справятся сами?

Большие игроки справятся сами, а для маленьких нужно выпускать методические рекомендации по принятию обязательного минимума мер, которые могут значительно повысить уровень их кибербезопасности. Роль объединений в данном вопросе не регуляторная, а просветительская.

???? ??? ?? ?????? ? ??????????? ??????? ???????????????

Читайте также:

«Вы не можете полностью защититься от кибератак»
«Любой случай с утечкой данных может поставить крест на бренде»
Интервью с Андреем Корельским, управляющим партнером КИАП

Хольгер Цшайге
«Киберпреступность не является проблемой IT»

ПРОГНОЗ РИСКОВ ДЛЯ БРИТАНСКИХ ЮРИСТОВ НА 2016-2017 ГГ.: РОСТ КИБЕРПРЕСТУПНОСТИ

ИНТЕРВЬЮ НОВОСТИ КОМПАНИЙ